

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

V.

ALAN BILL,

a/k/a Vem0r

a/k/a KingdomOfficial

Defendant.

Case No. 4:23-CR-714 RWS/NCC

**GOVERNMENT’S RESPONSE IN OPPOSITION  
TO DEFENDANT’S MOTIONS TO SUPPRESS EVIDENCE**

COMES NOW, the United States of America, by and through its attorneys, Sayler A. Fleming, United States Attorney for the Eastern District of Missouri, and Kyle T. Bateman, Assistant United States Attorney for said District, and responds in opposition to defendant Alan Bill's Motion to Suppress Evidence ([Doc. 98](#)) (the "Motion").

## Table of Contents

|      |  |    |
|------|--|----|
| I.   | Table of Authorities .....   | ii |
| II.  | Procedural Background .....  | 2  |
| III. | Relevant Facts .....   | 3  |
| A.   | Kingdom Market and the Defendant's Role as Administrator.....  | 3  |
| B.   | Searches of the Google Account.....  | 5  |
| C.   | The Defendant Travels to the United States .....   | 7  |
| D.   | The Defendant is Referred to Secondary Inspection and the Investigative Team<br>Obtains a Federal Search Warrant for His Devices .....   | 10 |
| E.   | The Defendant Voluntarily Agrees to Questioning by the Investigative Team.....   | 12 |
| IV.  | Argument.....  | 16 |
| A.   | The Defendant is Not Entitled to a <i>Franks</i> Hearing .....   | 16 |
| B.   | None of the Defendant's Statements at the New Jersey Airport Should be<br>Suppressed.....  | 19 |
| 1.   | The Defendant Was Not In Custody When CBPOs Performed a Routine Border<br>Inspection.....  | 20 |
| 2.   | The Defendant Was Not In Custody When He Voluntarily Joined Federal<br>Agents In An Open Conference Room And Waited For An Interpreter .....                                       | 21 |
| 3.   | The <i>Miranda</i> Warnings Provided to the Defendant Do Not Violate <i>Missouri v.</i><br><i>Seibert</i> and the Defendant's Post- <i>Miranda</i> Statements Are Admissible ..... | 24 |
| 4.   | The Defendant Knowingly, Intelligently and Voluntarily Waived His <i>Miranda</i><br>Rights .....   | 26 |
| C.   | Evidence Obtained from the Defendant's Devices Should Not Be Suppressed.....   | 27 |
| 1.   | The Search of the Defendant's Devices at the Airport Was Permissible Under<br>the Border Search Doctrine .....   | 28 |
| 2.   | The Devices Warrant Is Supported by Ample Probable Cause.....  | 33 |
| 3.   | The Device Search Warrant Is Sufficiently Particular and Is Not Overbroad ..   | 35 |
| D.   | The Google Warrants Should Not Be Suppressed .....   | 37 |
| 1.   | The Google Warrants Are Supported By Ample Probable Cause .....  | 37 |
| 2.   | The Google Warrants Are Sufficiently Particular and Are Not Overbroad .....  | 39 |
| V.   | Conclusion .....   | 40 |

## I. Table of Authorities

### Cases

|  |            |
|--|------------|
| <i>Alasaad v. Mayorkas</i> , 988 F.3d 8 (1st Cir. 2021) .....                      | 30, 32     |
| <i>California v. Beheler</i> , 463 U.S. 1121 (1983) .....                          | 21         |
| <i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018) .....                   | 30         |
| <i>Carrion v. Butler</i> , 835 F.3d 764 (7th Cir. 2016) .....                      | 27         |
| <i>Carroll v. United States</i> , 267 U.S. 132 (1925) .....                        | 28         |
| <i>Florida v. Harris</i> , 568 U.S. 237 (2013) .....                               | 33         |
| <i>Franks v. Delaware</i> , 438 U.S. 154 (1978) .....                              | 16         |
| <i>Illinois v. Gates</i> , 462 U.S. 213 (1983) .....                               | 33         |
| <i>Kentucky v. King</i> , 563 U.S. 452 (2011) .....                                | 35         |
| <i>Milliman v. Minnesota</i> , 774 F.2d 247 (8th Cir. 1985) .....                  | 36         |
| <i>Miranda v. Arizona</i> , 384 U.S. 436 (1966) .....                              | 26         |
| <i>Missouri v. Seibert</i> , 542 U.S. 600 (2004) .....                             | 19, 24, 25 |
| <i>Moran v. Burbine</i> , 475 U.S. 412 (1986) .....                                | 26         |
| <i>Riley v. California</i> , 573 U.S. 373 (2014) .....                             | 29         |
| <i>Stansbury v. California</i> , 511 U.S. 318 (1994) .....                         | 22         |
| <i>United States v. Aguilar</i> , 384 F.3d 520 (8th Cir. 2004) .....               | 25         |
| <i>United States v. Aldridge</i> , 664 F.3d 705 (8th Cir. 2011) .....              | 22         |
| <i>United States v. Allen</i> , 2018 WL 1726349 (D. Kan. Apr. 10, 2018) .....      | 36, 39     |
| <i>United States v. Axsom</i> , 289 F.3d 496 (8th Cir. 2002) .....                 | 22, 23     |
| <i>United States v. Black Bear</i> , 422 F.3d 658 (8th Cir. 2005) .....            | 25, 26     |
| <i>United States v. Blackwell</i> , 2018 WL 6804803 (D. Minn. Dec. 27, 2018) ..... | 20         |
| <i>United States v. Briones</i> , 390 F.3d 610 (8th Cir. 2004) .....               | 24         |
| <i>United States v. Buchanan</i> , 167 F.3d 1207 (8th Cir. 1999) .....             | 33, 38     |
| <i>United States v. Cano</i> , 934 F.3d 1002 (9th Cir. 2019) .....                 | 29, 31, 33 |
| <i>United States v. Castillo</i> , 70 F. 4th 894 (5th Cir. 2023) .....             | 30, 33     |
| <i>United States v. Castro-Higuero</i> , 473 F.3d 880 (8th Cir. 2007) .....        | 27         |
| <i>United States v. Coleman</i> , 909 F.3d 925 (8th Cir. 2018) .....               | 36         |
| <i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013) .....             | 31         |
| <i>United States v. Crisolis-Gonzalez</i> , 742 F.3d 830 (8th Cir. 2014) .....     | 23         |
| <i>United States v. Czichray</i> , 378 F.3d 822 (8th Cir. 2004) .....              | 23         |
| <i>United States v. Daigle</i> , 947 F.3d 1076 (8th Cir. 2020) .....               | 34, 38     |
| <i>United States v. Etheridge</i> , 165 F.3d 655 (8th Cir. 1999) .....             | 34         |
| <i>United States v. Fiorito</i> , 640 F.3d 338 (8th Cir. 2011) .....               | 36         |
| <i>United States v. Flores-Montano</i> , 541 U.S. 149 (2004) .....                 | 28         |
| <i>United States v. Gallardo</i> , 495 F.3d 982 (8th Cir. 2007) .....              | 26         |
| <i>United States v. Garcia</i> , 189 F. Supp. 3d 826 (S.D. Iowa 2016) .....        | 27         |
| <i>United States v. Gladney</i> , 48 F.3d 309 (8th Cir. 1995) .....                | 34         |
| <i>United States v. Green</i> , 954 F.3d 1119 (8th Cir. 2020) .....                | 34, 38     |
| <i>United States v. Griffin</i> , 922 F.2d 1343 (8th Cir. 1990) .....              | 22         |
| <i>United States v. Gust</i> , 471 F. 3d 144 (D.C. Cir. 2006) .....                | 33         |

|  |            |
|--|------------|
| <i>United States v. Hayes</i> , <a href="#">120 F.3d 739</a> (8th Cir. 1997) .....                   | 23         |
| <i>United States v. Hernandez-Hernandez</i> , <a href="#">384 F.3d 562</a> (8th Cir. 2004) .....     | 25         |
| <i>United States v. Horn</i> , <a href="#">187 F.3d 781</a> (8th Cir. 1999) .....                    | 34, 35     |
| <i>United States v. Huether</i> , <a href="#">673 F.3d 789</a> (8th Cir. 2012) .....                 | 22         |
| <i>United States v. Ickes</i> , <a href="#">393 F.3d 501</a> (4th Cir. 2005) .....                   | 30         |
| <i>United States v. Intarathong</i> , <a href="#">2021 WL 8082965</a> (D. Minn. Dec. 30, 2021) ..... | 20         |
| <i>United States v. Jones</i> , <a href="#">70 F.4th 1109</a> (8th Cir. 2023) .....                  | 25         |
| <i>United States v. Layne</i> , <a href="#">973 F.2d 1417</a> (8th Cir. 1992) .....                  | 20         |
| <i>United States v. Laynes</i> , <a href="#">481 F. Supp. 3d 657</a> (S.D. Ohio 2020) .....          | 29         |
| <i>United States v. LeBrun</i> , <a href="#">363 F.3d 715</a> (8th Cir. 2004) .....                  | 21         |
| <i>United States v. Levy</i> , <a href="#">803 F.3d 120</a> (2d Cir. 2015) .....                     | 33         |
| <i>United States v. Linarez-Delgado</i> , <a href="#">259 F. App'x 506</a> (3d Cir. 2007) .....      | 30         |
| <i>United States v. Lind</i> , <a href="#">542 F.2d 598</a> (2d Cir. 1976) .....                     | 27         |
| <i>United States v. Mendez</i> , <a href="#">103 F.4th 1303</a> (7th Cir. 2024) .....                | 21, 32     |
| <i>United States v. Molina-Isidoro</i> , <a href="#">884 F.3d 287</a> (5th Cir. 2018) .....          | 31         |
| <i>United States v. Montoya de Hernandez</i> , <a href="#">473 U.S. 531</a> (1985) .....             | 28         |
| <i>United States v. Nieman</i> , <a href="#">520 F.3d 834</a> (8th Cir. 2008) .....                  | 36         |
| <i>United States v. Notman</i> , <a href="#">831 F.3d 1084</a> (8th Cir. 2016) .....                 | 33         |
| <i>United States v. Ollie</i> , <a href="#">442 F.3d 1135</a> (8th Cir. 2006) .....                  | 22, 25     |
| <i>United States v. Oropesa</i> , <a href="#">316 F.3d 762</a> (8th Cir. 2003) .....                 | 33         |
| <i>United States v. Oyekan</i> , <a href="#">786 F.2d 832</a> (8th Cir. 1986) .....                  | 20         |
| <i>United States v. Peters</i> , <a href="#">92 F.3d 768</a> (8th Cir. 1996) .....                   | 36         |
| <i>United States v. Ramsey</i> , <a href="#">431 U.S. 606</a> (1977) .....                           | 28, 32     |
| <i>United States v. Saboonchi</i> , <a href="#">48 F. Supp. 3d 815</a> (D. Md. 2014) .....           | 30         |
| <i>United States v. Sigillito</i> , <a href="#">759 F.3d 913</a> (8th Cir. 2014) .....               | 36         |
| <i>United States v. Skaggs</i> , <a href="#">25 F.4th 494</a> (7th Cir. 2022) .....                  | 31         |
| <i>United States v. Solomon</i> , <a href="#">432 F.3d 824</a> (8th Cir. 2005) .....                 | 33, 38     |
| <i>United States v. Stewart</i> , <a href="#">729 F.3d 517</a> (6th Cir. 2013) .....                 | 30         |
| <i>United States v. Strand</i> , <a href="#">761 F.2d 449</a> (8th Cir. 1985) .....                  | 35         |
| <i>United States v. Summage</i> , <a href="#">481 F.3d 1075</a> (8th Cir. 2007) .....                | 35         |
| <i>United States v. Syslo</i> , <a href="#">303 F.3d 860</a> (8th Cir. 2002) .....                   | 26         |
| <i>United States v. Touse</i> , <a href="#">890 F.3d 1227</a> (11th Cir. 2018) .....                 | 30, 31, 32 |
| <i>United States v. Treanton</i> , <a href="#">57 F.4th 638</a> (8th Cir. 2023) .....                | 22         |
| <i>United States v. Udofot</i> , <a href="#">711 F.2d 831</a> (8th Cir. 1983) .....                  | 30         |
| <i>United States v. Ulbricht</i> , <a href="#">858 F.3d 71</a> (2d Cir. 2017) .....                  | 39         |
| <i>United States v. Unpradit</i> , <a href="#">2018 WL 4483682</a> (D. Minn. May 14, 2018) .....     | 21         |
| <i>United States v. Walker</i> , <a href="#">518 F.3d 983</a> (8th Cir. 2008) .....                  | 25         |
| <i>United States v. Wanjiku</i> , <a href="#">919 F.3d 472</a> (7th Cir. 2019) .....                 | 30, 31     |
| <i>United States v. Warford</i> , <a href="#">439 F.3d 836</a> (8th Cir. 2006) .....                 | 33         |
| <i>United States v. Williams</i> , <a href="#">477 F.3d 554</a> (8th Cir. 2007) .....                | 16         |
| <i>United States v. Williams</i> , <a href="#">10 F.3d 590</a> (8th Cir. 1993) .....                 | 33         |
| <i>United States v. Williams</i> , <a href="#">942 F.3d 1187</a> (10th Cir. 2019) .....              | 31         |
| <i>United States v. Wise</i> , <a href="#">588 F.3d 531</a> (8th Cir. 2009) .....                    | 25         |
| <i>United States v. Xiang</i> , <a href="#">67 F.4th 895</a> (8th Cir. 2023) .....                   | 29, 32, 33 |

**Statutes**

|   |                 |
|---|-----------------|
| <a href="#"><u>8 U.S.C. § 1225(a)(3)</u></a> .....  | 20              |
| <a href="#"><u>8 U.S.C. § 1225(a)(5)</u></a> .....  | 20              |
| <a href="#"><u>8 U.S.C. § 1357(c)</u></a> .....     | 20              |
| <a href="#"><u>18 U.S.C. § 1028(a)(7)</u></a> ..... | 2               |
| <a href="#"><u>18 U.S.C. § 1028(f)</u></a> .....    | 2               |
| <a href="#"><u>18 U.S.C. § 1028A</u></a> .....      | 2               |
| <a href="#"><u>18 U.S.C. § 1544</u></a> .....       | 2               |
| <a href="#"><u>18 U.S.C. § 1956(h)</u></a> .....    | 2               |
| <a href="#"><u>18 U.S.C. § 2703(d)</u></a> .....    | 5, 6, 38        |
| <a href="#"><u>18 U.S.C. § 371</u></a> .....        | 6, 7, 12, 37    |
| <a href="#"><u>19 U.S.C. § 482</u></a> .....        | 28              |
| <a href="#"><u>19 U.S.C. § 1582</u></a> .....       | 28              |
| <a href="#"><u>21 U.S.C. § 841</u></a> .....        | 6, 7, 12, 37    |
| <a href="#"><u>21 U.S.C. § 841(a)(1)</u></a> .....  | 2               |
| <a href="#"><u>21 U.S.C. § 846</u></a> .....        | 2, 6, 7, 12, 37 |

## **II. Procedural Background**

On December 14, 2023, the defendant Alan Bill was arrested at the Newark Liberty International (EWR) Airport in the District of New Jersey after he was charged by criminal complaint. Doc. 1.

On December 20, 2023, a federal grand jury in the Eastern District of Missouri returned a ten-count Indictment against the defendant, including: one count of conspiracy to distribute controlled substances in violation of 21 U.S.C. § 846 (Count 1); four counts of distribution of a controlled substance in violation of 21 U.S.C. § 841(a)(1) (Counts 2, 3, 4, 5); one count of conspiracy to commit identity theft in violation of 18 U.S.C. § 1028(f) (Count 6); one count of identity theft in violation of 18 U.S.C. § 1028(a)(7) and (1) (Count 7); one count of aggravated identity theft in violation of 18 U.S.C. § 1028A (Count 8); one count of misuse of passport in violation of 18 U.S.C. § 1544 (Count 9); and one count of money laundering conspiracy in violation of 18 U.S.C. § 1956(h) (Count 10). Doc. 11.

On May 22, 2024, the defendant filed a motion to suppress the following evidence: (i) all statements made by the defendant at the EWR airport; (ii) all evidence obtained through the search of the defendant's devices that were seized from him at the EWR airport; and (iii) all evidence obtained through the searches of his Google account *Alan.vs.Bill@gmail.com* (the "Google Account"), conducted pursuant to Cause Nos. 4:23-mj-7338 and 4:23-mj-3376 NCC SPM.<sup>1</sup> Doc. 98.

---

<sup>1</sup> The Motion does not specifically state which of these two warrants that the defendant moves to suppress. As such, the Government construes the Motion as seeking to suppress both warrants.

### **III. Relevant Facts**<sup>2</sup>

In approximately May 2022, the Government began investigating Kingdom Market (“Kingdom”) and its administrators. This investigation was conducted by numerous federal and state agencies, including but not limited to, the Internal Revenue Service Criminal Investigations (IRS-CI), the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the Drug Enforcement Administration (DEA), United States Postal Inspectors Service (USPIS), and Diplomatic Security Services (DSS) (hereinafter the “Investigative Team”).

#### **A. Kingdom Market and the Defendant’s Role as Administrator**

Between March 2021 and December 2023, Kingdom operated as an online darknet marketplace that enabled users to buy and sell illegal drugs and other illicit goods and services, including stolen financial information, fraudulent identification documents, counterfeit currencies, computer malware, and fraudulent identity documents. These items and services were offered for sale and purchase by and through cryptocurrency; specifically, Bitcoin, Monero (XMR), and Litecoin. Kingdom allowed individuals to pay for illegal goods and services by making a cryptocurrency payment to an escrow account that was controlled by Kingdom administrators.

Kingdom administrators publicly advertised that they began development of the site in the summer of 2020. However, the marketplace did not open for public use until March 2021. On December 16, 2023, German and Swiss law enforcement, working with the Investigative Team, successfully shut down Kingdom.

Over the course of the investigation, the Investigative Team discovered that the defendant, who is a Slovakian national, had numerous connections to Kingdom, its operations and

---

<sup>2</sup> This is a summary of the information that the Government anticipates will be presented at the evidentiary hearing and does not constitute a fixed theory of proof.

cryptocurrency transactions. For example, the Investigative Team first discovered that a specific IP address resolving to Slovakia (“IP Address 1”) was used to access Kingdom’s Reddit account “u/KingdomOfficial,” which was listed as a moderator and administrator of the Kingdom subreddit (r/KingdomOfficial). This u/KingdomOfficial account made numerous postings regarding the administration of Kingdom, including to provide users with instructions on how to access Kingdom. IP Address 1 was also used to access the defendant’s cryptocurrency account with Bittrex, his cryptocurrency account with Binance, his email address (*Alan.vs.Bill@gmail.com*) and for the defendant to apply for the United States’ Visa Waiver Program (VWP) in January 2023.

In August 2023, United States Magistrate Judge Shirley P. Mensah signed a search warrant (Cause No. 4:23-MJ-7279 SPM) for Kingdom’s Reddit accounts r/kingdomofficial, u/kingdomofficial, u/ohlongjohnsonKM, and u/papinian3. These accounts were listed as being the official subreddit of Kingdom and the moderators of Kingdom. In a review of responsive records from Reddit, the Investigative Team discovered private messages wherein u/OhLongJohnsonKM requested graphic design assistance from another individual for a new logo and banner advertisements for Kingdom. The messages contained dates, amounts, and the cryptocurrency payment address of the graphic artist and showed that the graphic artist was paid in at least three cryptocurrency transactions between March 3, 2023, and May 4, 2023. The Investigative Team reviewed open-source records for the graphic artist’s payment address and observed that the above referenced payments came from a cryptocurrency address that had previously been funded by the defendant’s Binance account and by other transactions associated with IP Address 1.

The Investigative Team was also able to trace specific cryptocurrency transactions from a cluster or group of cryptocurrency addresses used by Kingdom to the defendant’s accounts with Bittrex and Binance. The timing and amount of these transactions led the Investigative Team to believe that they represent payments to an administrator of Kingdom. For example, one of these



transactions, which occurred in July 2022, was a transfer of 2.19999968 BTC (approximately \$42,000 at the time) that is inconsistent with typical payments between buyers and vendors. In addition, another of these transactions, which occurred in November 2021, was a transfer of Litecoin that appears to be a test transaction to ensure that Kingdom was able to accept and hold Litecoin payments.

## **B. Searches of the Google Account**

On July 13, 2023, United States Magistrate Judge Mensah signed an order pursuant to [18 U.S.C. § 2703\(d\)](#) for transactional non-content records associated with the Google Account. This account was used by the defendant on both his Bittrex and Binance accounts.

Thereafter, the Investigative Team sought and received two separate search warrants for the Google Account (together, the “Google Warrants”):

- On September 14, 2023, United States Magistrate Judge Shirley P. Mensah signed a search warrant (4:23-mj-7338 SPM) for the Google Account (the “First Google Warrant”); and
- On December 8, 2023, United States Magistrate Judge Noelle C. Collins signed a search warrant (Cause No. 4:23-mj-3376 NCC) for the Google Account (the “Second Google Warrant”).

The First Google Warrant was supported by an application and affidavit of IRS-CI Special Agent Joifrita. The affidavit for the First Google Warrant provided background on the dark web and cryptocurrency (paragraphs 21 to 26) and information about the investigation into Kingdom (paragraphs 27 to 39). The affidavit then described specific links between Kingdom cryptocurrency accounts and two of the defendant’s cryptocurrency accounts, both of which listed the defendant’s Google account as the associated email address (paragraphs 40 to 45). The affidavit explained that the defendant used his Google account on travel records to the United

States in 2018 (paragraph 46). The affidavit then explained that the results from a 18 U.S.C. § 2703(d) order included non-content records showing that the Google Account had received numerous email messages from cryptocurrency services such as crypto.com, coinstats.app and LocalMonero (paragraphs 49 to 52). Finally, the affidavit described in detail specific transactions wherein the defendant's cryptocurrency accounts were used to make a payment from Kingdom to a third-party service provider (paragraphs 53 to 58). The warrant included an Attachment B that limited the information to be seized by the Government to "fruits, contraband, evidence, and instrumentalities of violations" of 18 U.S.C. §§ 371, 1028, 1956 and 1957 and 21 U.S.C. §§ 841 and 846, occurring from July 1, 2020, and September 13, 2023, or relating to the defendant and pertaining to 23 specific matters.

Similarly, the Second Google Warrant was supported by an application and affidavit from IRS-CI SA Joifrita. The affidavit for the Second Google Warrant included the same information as set forth in the affidavit for the First Google Warrant, but also included additional information related to the results of the first search (paragraphs 60 to 74). Specifically, the affidavit stated that results from the first search showed: images and videos that included the name "Vend0r" on them (paragraph 62); a video file showing an individual performing administrative functions on Kingdom (paragraphs 63 to 67); internet image and keyword searches for "kingdom Market", "server housing" and "Litecoin icon" before Kingdom existed (paragraph 69); and numerous files showing recovery information and seed phrases for cryptocurrency accounts, IP masking tools and encrypted cloud storage and file hosting services, including ones that have a direct link to Kingdom (paragraphs 70 to 72). The warrant included an Attachment B that limited the information to be seized by the Government to "fruits, contraband, evidence, and instrumentalities of violations" of

18 U.S.C. §§ 371, 1028, 1956 and 1957 and 21 U.S.C. §§ 841 and 846 occurring from September 13, 2024, to present, or relating to the defendant and pertaining to 23 specific matters.

Both Google Warrants included an Attachment B that provided limitations on the evidence to be seized. The Google Warrants both had temporal restrictions, restrictions related to the investigated crimes, and restrictions related to the defendant. The Google Warrants also stated that the evidence to be seized was limited to categories such as: evidence concerning the operation or control of websites used to facilitate the distribution of illegal drugs; evidence related to the use of monikers “vend0r” and “kingdommarketofficial”; evidence related to the use of PGP private keys; and evidence related to the use of cryptocurrency.

### **C. The Defendant Travels to the United States**

During the course of the investigation, and through Department of Homeland Security (DHS) database research conducted by HSI Special Agent Nolan Kraft, the Investigative Team discovered that the defendant travelled to the United States as a visitor for pleasure in January 2023. To enter the United States, the defendant relied upon the Visa Waiver Program (VWP),<sup>3</sup> which allows citizens of certain countries to enter the United States without a visa issued by the U.S. Department of State.

On or about September 12, 2023, HSI SA Kraft created a DHS agency-internal investigative person/subject record containing the defendant’s biographical information. This record and its data are a mechanism to share information across other DHS component agencies,

---

<sup>3</sup> The Visa Waiver Program (VWP), administered by DHS in consultation with the State Department, permits citizens of 41 countries (including Slovakia) to travel to the United States for business or tourism for stays of up to 90 days without a visa. As part of a diplomatic reciprocity function, those 41 countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes.

namely United States Customs and Border Protection (CBP). Within that record, HSI SA Kraft authored brief remarks summarizing the defendant's suspected involvement in cross-border criminal activity.

On or about October 3, 2023, HSI SA Kraft reviewed DHS database records and learned that the defendant had submitted a new VWP application, suggesting that he was planning to travel to the United States. As a result, HSI SA Kraft updated his remarks in the defendant's person/subject record to reflect the defendant's potential upcoming travel to the United States and to request that any U.S. Customs and Border Protection officer ("CBPO")<sup>4</sup> contact HSI SA Kraft when the subject of the record (the defendant) scheduled future inbound international travel to the United States.<sup>5</sup> Additionally, HSI SA Kraft notified CBP that the Investigative Team would like to coordinate directly with CBP if the defendant scheduled future travel to the United States. At this time, the Investigative Team did not know whether the defendant was planning to travel to the United States.

On December 11, 2023, HSI SA Kraft learned that CBP officer(s) had viewed the person/subject record for the defendant. Subsequently, HSI SA Kraft learned from DHS databases and by speaking with CBP officer(s) that the defendant had ticketed travel from Vienna, Austria, to EWR airport on Thursday, December 14, 2023, via Austrian Airlines, and was set to arrive at 2:15 pm Eastern Time. According to the ticket, the defendant was travelling with V.V. However,

---

<sup>4</sup> CBP is a DHS component agency, comprised primarily of uniformed law enforcement officers (CBPOs) charged with securing the borders, enforcing federal law at the United States Ports of Entry (POE) and preventing transnational crime.

<sup>5</sup> Through several automated systems, CBP receives advanced passenger data from airlines so that CBP officers may conduct vetting of inbound international commercial air and/or sea travelers prior to their arrival. During this process, CBP may contact other DHS components or other law enforcement agencies to assist in determining admissibility of passengers scheduled to arrive at a United States Port of Entry (POE).

CBP further notified SA Kraft that, upon additional vetting, CBP determined that the defendant was potentially ineligible for the VWP at this time since he did not accurately report historical travel to a restricted country (Cuba). HSI SA Kraft was unable to confirm or access historical travel information relating to Cuba at that time.

On December 12, 2023, HSI SA Kraft sent a collateral investigative request to HSI Newark Special Agent Anthony Chen. The request was subsequently handled jointly by HSI SA Chen and CBP Task Force Officer (TFO) Richard Moses. HSI SA Kraft requested that CBPOs refer the defendant to secondary inspection upon his arrival at Newark airport where he would be questioned, and his luggage could be subjected to a border search. In addition, HSI SA Kraft advised CBPOs that he expected that the defendant's electronic devices would likely contain a great deal of technical information related to the criminal investigation. Pursuant to this conversation, CBP concluded that they would likely need assistance from the Investigative Team to inspect the devices.<sup>6</sup>

On December 13, 2023, HSI SA Kraft, FBI SA Ogurek, and IRS-CI SA Joifrita travelled to Newark, New Jersey, to be available to CBP, should CBP require either technical or subject matter assistance during its border search of the defendant's electronic devices.

As described above, CBPOs assigned to the vetting process of VWP applicants determined that the defendant may be ineligible for a visa waiver. Accordingly, on December 14, 2023, the United States Attorney for the Eastern District of Missouri sent a letter to the Acting Port Director for the Port of New York/Newark. In this letter, the U.S. Attorney notified the Acting Port Director

---

<sup>6</sup> CBP policy governing border searches of electronic devices recognizes that there are situations where CBP officers may require assistance—either subject matter or technical assistance—to complete a border search of electronic devices. CBP Directive No. 3340-049A, *Border Searches of Electronic Devices*, § 5.4.2 (Jan. 4, 2018).

that the defendant had been identified as an administrator of an online darknet marketplace that allows users to buy and sell drugs, stolen/fraudulent passports, stolen identities, and other illicit items. The U.S. Attorney further requested that the Acting Port Director grant Port Parole to the defendant allowing him permission to enter the United States.

**D. The Defendant is Referred to Secondary Inspection and the Investigative Team Obtains a Federal Search Warrant for His Devices**

On December 14, 2023, at approximately 2:15 pm Eastern Time, the defendant and V.V. arrived in the United States at EWR airport. Upon arrival, the defendant and V.V. provided their passports to a CBPO at primary inspection.

CBPOs referred the defendant and V.V. to secondary inspection and they were escorted down some stairs from the primary inspection area to an open area. At the secondary inspection area, upon questioning of his travels, the defendant told CBPOs that he and V.V. were travelling to the United States on their honeymoon. CBPOs then searched the defendant's luggage. Within the defendant's luggage, the CBPOs discovered an Apple iPhone 15 cellular phone, a RealMe RMX2155 cellular phone, a Dell XPS laptop, a Samsung 256 MB thumb drive, and a Trezor Model T device.<sup>7</sup> Upon request, the defendant provided the passwords for his cellular phones and laptop computer to CBPOs. CBPOs performed a basic search of these devices and discovered encrypted communications relating to Kingdom Market.

The CBPOs then provided the defendant's devices to the Investigative Team. At approximately 4:26 pm Eastern Time, HSI SA Kraft applied for and received a federal search warrant from United States Magistrate Judge Mark Hammer, District of New Jersey (Cause No.

---

<sup>7</sup> A Trezor is a type of "hardware wallet," which is a physical device resembling a USB thumb drive that is used to securely store cryptocurrency private keys in an offline capacity for enhanced security. In essence, a Trezor is a secure vault that holds passwords to access and spend cryptocurrency.

4:23-mj-10334 MAH) authorizing the seizure and examination of the defendant's two cell phones, his laptop computer and USB thumb drive, and the extraction from that property of electronically stored information (hereinafter the "Devices Warrant").

The Devices Warrant was supported by an application and affidavit of HSI SA Kraft. The affidavit for the Devices Warrant provided information about the investigation into Kingdom (paragraphs 11 to 18), described how Kingdom administrators used various online platforms to promote business and otherwise keep operations running (paragraphs 19 to 28), and listed specific controlled buys on Kingdom (paragraph 29). The affidavit then described links between Kingdom and the defendant, including: an IP address used to access Kingdom's reddit account was also used to access the defendant's cryptocurrency accounts, which received large amounts of cryptocurrency from Kingdom (paragraphs 30 to 44); large, unexplained cash deposits were made into the defendant's various bank accounts (paragraphs 45 to 49); the results of the search of the defendant's Google account revealed significant links to Kingdom, its back-end infrastructure and cryptocurrency accounts (paragraph 64); the results of the search of Kingdom's Reddit accounts showed direct links to the defendant (paragraphs 65 to 69); the results of the search of the defendant's Apple iCloud account showed that defendant utilized numerous encrypted communication applications (paragraphs 70 to 75). The affidavit further described that defendant traveled extensively around the world in 2022 and 2023 (paragraph 76) and that he used an Apple iPhone on the AT&T network when he was in the United States in January 2023, including at a time when Kingdom had experienced a DDoS attack and was actively posting messages to its users (paragraph 80). The affidavit described how the seized devices were all capable of accessing the internet and the programs known to be used to operate Kingdom, and would be necessary to ensure Kingdom's continued operations (paragraphs 80 and 82). The warrant included an Attachment B

that limited the information to be seized by the Government to records that relate to violations of 18 U.S.C. §§ 371, 1028, 1029, 1543, 1956 and 1957 and 21 U.S.C. §§ 841 and 846, involving the defendant from January 2020 to present.

Upon obtaining the Devices Warrant, the defendant's electronic devices were turned over to HSI Newark computer forensic agents and taken to the Forensic Computer Laboratory at the HSI Newark field office.

A special agent with HSI told the defendant that they needed to perform a forensic examination of the defendant's electronic devices, that such procedure would take some time, and that he could retrieve the devices the following morning. The defendant was provided a DHS Form 6051D (Detention Notice and Custody Receipt for Detained Property) that listed the devices and provided information as to how the defendant could retrieve the devices.

**E. The Defendant Voluntarily Agrees to Questioning by the Investigative Team**

Both the defendant and V.V. were released from secondary inspection and were told they were free to go. At approximately 4:46 pm Eastern Time, the defendant and V.V. were allowed to pass through the CBP secured area and enter the United States in the EWR airport. The Investigative Team maintained physical surveillance of the defendant.

At approximately 5:15 pm Eastern Time, FBI SA Ogurek presented an affidavit to United States Magistrate Judge Joseph S. Dueker for the Eastern District of Missouri seeking a complaint and arrest warrant for the defendant. Cause 4:23-mj-2288 JSD. Judge Dueker signed the complaint and warrant.

During this time, the defendant and V.V. were observed sitting in the terminal of the EWR airport. At approximately 5:50 pm Eastern Time, FBI SA Ogurek, HSI SA Kraft, TFO Moses, HSI SA Elena Parra-Perrez, and a uniformed CBPO approached the defendant while he was seated



in the terminal. The defendant was asked if he was willing to speak in a non-public area of the airport. The defendant agreed and followed the agents through several doors to a large open room with a conference table. The door to the room remained open at all times. The defendant was not handcuffed.

The defendant sat at the conference table. Also seated at the table were three, plain-clothed members of the Investigative Team: HSI SA Kraft, FBI SA Ogurek and IRS-CI SA Joifrita. None of these agents displayed a firearm to the defendant. During the course of the interview, several CBPOs in plain clothes walked in and out of the room; none of them participated in the interview.

IRS-CI SA Joifrita recorded the audio of this interview using an audio recording device.<sup>8</sup> The audio recording began within approximately 30 seconds of the beginning of the encounter with the defendant.

At the beginning of the interview, HSI SA Kraft attempted to communicate with the defendant using the Google translation application on his cellular phone. This application provided real time translation to and from English and Slovakian. At the beginning of the recording, the defendant stated that he could understand the translations being played for him through the Google translation application.

Approximately 1 minute into the recording, HSI SA Kraft offered water and any needed medication to the defendant. HSI SA Kraft also told the defendant that V.V. would stay upstairs while agents spoke to the defendant.

Approximately 3 minutes into the recording, the defendant stated that his colleague uses the defendant's phones and laptop. This statement was not made in response to any question by

---

<sup>8</sup> The audio recording is approximately 2 hours and 57 minutes long.

agents. HSI SA Kraft told the defendant to wait until they can find an interpreter. The defendant responded that V.V. could be the translator for them, but HSI SA Kraft said that he prefers to use a different interpreter.

Approximately 6 minutes into the recording, the defendant asked the agents why he was there. HSI SA Kraft responded that they want assistance with things going on in Slovakia. The defendant then asked how he can help. HSI SA Kraft then asked the defendant if he had any idea why the agents would want to talk with him, and the defendant responded no.

Approximately 8 minutes into the recording, HSI SA Kraft asked the defendant about his electronic devices, who they belong to, and why the defendant had them with him. The defendant provided responses to these questions.

Approximately 12 minutes into the recording, HSI SA Kraft told the defendant that he did not want to continue without an interpreter. After this point, the agents did not ask any further questions of the defendant and there was a prolonged break during which agents were trying to find an interpreter.

Approximately 21 minutes into the recording, the defendant told agents that he understood the Czech language. The agents responded that might be helpful in their efforts to find an interpreter.

Approximately 38 minutes into the recording, while agents were waiting for an interpreter, the defendant asked why he is there, whether he can make a telephone call and whether he would be able to leave with his wife (V.V.). The defendant also stated that he did not commit any crimes in the United States. In response, HSI SA Kraft told the defendant that he was allowed to make a phone call and that they would talk more once they found an interpreter.

Approximately 43 minutes into the recording, the defendant asked to use the bathroom and he was allowed to do so.

Approximately 48 minutes into the recording, FBI SA Ogurek asked the defendant if he understood Czech and the defendant responded that he did.

Approximately 54 minutes into the recording, the defendant again said that he understood Czech.

FBI SA Ogurek then located an FBI employee, Ms. Zuzanna Arata, who could speak both Czech and English. FBI SA Ogurek called Ms. Arata and placed her on speakerphone so that the defendant and the Investigative Team could hear her.

Approximately 1 hour and 16 minutes into the recording, the interpreter began to translate the interview. Before proceeding with any questions, FBI SA Ogurek read the defendant his *Miranda* rights through the interpreter. The defendant stated that he understood his rights and would agree to speak to agents. The defendant also signed a written *Miranda* waiver form after it was translated to him.

Approximately 2 hours and 39 minutes into the recording, FBI SA Ogurek told the defendant that he was being placed under arrest and will be transported to jail. The defendant asked about medications in his luggage, whether he could speak to V.V. and whether he could make a phone call.

Approximately 2 hours and 44 minutes in the recording, the defendant stated that he would like to speak to an attorney.

## IV. Argument

### A. The Defendant is Not Entitled to a *Franks* Hearing

In his Motion, the defendant seeks a hearing pursuant to *Franks v. Delaware*, [438 U.S. 154](#) (1978) related to the Google Warrants. On July 12, 2024, the Government filed a motion asking that this Court make a finding that the defendant is not entitled to a *Franks* hearing. [Doc. 118](#). The Court has not yet ruled on this motion. However, in order for the parties to properly prepare for an evidentiary hearing, the Government here reasserts its position that the defendant has not met his burden entitling him to a *Franks* hearing.

In limited circumstances, a defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination. *Franks*, [438 U.S. at 155-56](#). The Eighth Circuit has held that a “defendant may only receive ‘a *Franks* hearing...after making a substantial preliminary showing’ that the warrant’s issuing judge relied on statements in an affidavit that were false or were ‘omissions made knowingly and intentionally or with reckless disregard for the truth.’” *United States v. Mayweather*, [993 F.3d 1035, 1043](#) (8th Cir. 2021) (quoting *United States v. El-Alamin*, [574 F.3d 915, 924](#) (8th Cir. 2009)) (emphasis added). This is a requirement that is “not easily met.” *United States v. Gabrio*, [295 F.3d 880, 883](#) (8th Cir. 2002) (citation omitted).

This preliminary showing “requires a defendant to offer specific allegations along with supporting affidavits or similarly reliable statements.” *Mayweather*, [993 F.3d at 1043](#) (quoting *United States v. Gonzalez*, [781 F.3d 422, 430](#) (8th Cir. 2015)) (emphasis added). There is a presumption of validity with respect to the affidavit and the challenger’s attack “must be more than conclusory.” *United States v. Williams*, [477 F.3d 554, 558](#) (8th Cir. 2007) (quoting *Franks*, [438 U.S. at 171](#)). The defendant must then show that the affidavit would not establish probable cause

if the allegedly false information is ignored or the omitted information is supplemented. *United States v. Reinholz*, [245 F.3d 765, 774](#) (8th Cir.2001) (citation omitted).

The defendant makes conclusory allegations that, as to the Devices Warrant, HSI SA Kraft “secured a warrant ... based on false allegations that [defendant] is the administrator of [Kingdom].” Motion, at 26. The defendant further alleges that HSI SA Kraft “failed to disclose readily available evidence that his statements and conclusions are based on assumptions and extremely unreliable technical data.” *Id.* Similarly, the defendant makes conclusory allegations that, as to the Google Warrants, IRS-CI SA Joifrita “fails to mention that ‘clustering’ used by the IRS is an extremely unreliable method of identification of cryptocurrency addresses” and that SA Joifrita “simply misled the Magistrate to solicit issuance of search warrant.” Motion, at 36-7. The defendant further claims that the information in SA Joifrita’s affidavits “was not only misleading and incomplete, but it was also highly unreliable conclusions based on assumptions and not scientific research.” *Id.* at 40.

In support of such allegations, the defendant provides a report authored by Mr. Eduard Jenco, that is dated March 22, 2024 (“Jenco Report”). *See* Motion, at Exhibit A. In making his conclusions, Mr. Jenco states that he relied upon (i) the affidavit of FBI SA Ogurek that accompanied the criminal complaint ([Doc. 2](#)), (ii) various court documents from December 2023, (iii) the Indictment, and (iv) a “preliminary review” of discovery materials provided by the U.S. Attorney’s Office four days earlier on March 18, 2024. *See* Motion, at Exhibit A, pages 5-6. That is, Mr. Jenco did not even review the Devices Warrant or the Google Warrants before coming to his conclusions.<sup>9</sup> Instead, Mr. Jenco’s conclusions are based upon his review of the complaint

---

<sup>9</sup> The March 18 discovery production referenced by Mr. Jenco was a re-production of Production 1, which includes records related to cryptocurrency accounts, Google accounts and bank records. The Devices Warrant and Google Warrants, including their corresponding affidavits, were not

affidavit from FBI SA Ogurek (who was not the affiant on any of the challenged warrants) and does not even directly address any of the challenged warrants. On this basis alone, the *Franks* hearing request should be denied.

In any event, the defendant's request for a *Franks* hearing is based on his claims that (i) the third-party blockchain-analysis tool used by the Government is unreliable, and (ii) the defendant's use of the TOR network somehow wrongly caused his IP address (IP Address 1) to be associated with Kingdom. The Government believes that the Jenco Report is flawed in many respects and, should this matter proceed to trial, the Government could introduce expert testimony that controverts the premises and conclusions of Mr. Jenco. The Government anticipates that at the time of trial, it would call multiple experts to address the issues raised in the Jenco Report. But a *Franks* hearing is not the proper forum for conflicting expert testimony. *See United States v. Wolfe*, No. 4:14CR152 RWS/NCC, [2016 WL 8310382](#), at \*4 (E.D. Mo. Dec. 14, 2016), *report and recommendation adopted*, No. 4:14 CR 152 RWS-5, [2017 WL 713033](#) (E.D. Mo. Feb. 23, 2017) (finding that the law does not require affiants of search warrants to be scientific experts and the defendant is not entitled to a *Daubert* hearing by way of a *Franks* hearing).

That is because, even if this Court were to accept as true the defendant's false premises that the Government's forensic tools are unreliable or the TOR network impacted the reporting of the defendant's IP address, those findings do not entitle the defendant to a *Franks* hearing. The defendant must also show that (i) SA Kraft and/or SA Joifrita had personal knowledge that the blockchain-analysis tool produced incorrect results and/or that the TOR network caused the wrong IP address to be reported in various circumstances; and (ii) SA Kraft and/or SA Joifrita intentionally withheld these facts in order to mislead the Court. The defendant has not introduced

---

produced to the defendant until March 29, 2024, after Mr. Jenco submitted his report.

any evidence to support either showing. In fact, as will be made clear at trial, evidence from Kingdom's servers fully verify and confirm the findings from the Government's forensic tools.

Based on the foregoing, the defendant does not make any showing that either SA Kraft or SA Joifrita *knowingly* made any false statements in their affidavits. The defendant must provide some evidence showing that either SA Kraft or SA Joifrita (or both) knowingly made a false statement in their affidavit. *See United States v. Crissler*, [539 F.3d 831, 833](#) (8th Cir. 2008) (denying *Franks* hearing where defendant made no offer of proof that the alleged statements or omissions were made intentionally or recklessly). The defendant has not done so here, and this Court should deny the defendant's request to conduct a *Franks* hearing as to both HSI SA Kraft or IRS-CI SA Joifrita.

**B. None of the Defendant's Statements at the New Jersey Airport Should be Suppressed**

Without identifying any particular statement that the defendant seeks to suppress, the defendant appears to argue that he was in custody from the moment he was approached by CBPOs as part of his border inspection.<sup>10</sup> *See* Motion, at 5. Thus, the Government's response assumes that the defendant seeks to suppress (i) statements that he made to CBPOs during the secondary inspection; (ii) statements that he made to members of the Investigative Team prior to receiving *Miranda* warnings (which encompass approximately the first 1 hour and 16 minutes of this encounter); and (iii) statements that he made to members of the Investigative Team after he received *Miranda* warning (which encompasses approximately 1 hour and 16 minutes into the encounter until his arrest). The defendant further argues that he was improperly subjected to a "two step interrogation" in violation of *Missouri v. Seibert*. *Id.* at 6. The defendant then argues

---

<sup>10</sup> The defendant mistakenly believes that the CBPOs who conducted a secondary inspection pursuant to the border search doctrine were FBI agents.

that his *Miranda* waiver was invalid because it was not made knowingly, intelligently and voluntarily. *Id.* at 8.

**1. The Defendant Was Not In Custody When CBPOs Performed a Routine Border Inspection**

There is well-established statutory authority for CBPOs to ask questions of individuals who are attempting to enter the United States. *See, e.g.,* [8 U.S.C. § 1225\(a\)\(3\)](#) (“All aliens...who are applicants for admission or otherwise seeking admission or readmission to or transit through the United States shall be inspected by immigration officers.”); [8 U.S.C. § 1225\(a\)\(5\)](#) (“An applicant for admission may be required to state under oath any information sought by an immigration officer regarding the purposes and intentions of the applicant in seeking admission to the United States, including the applicant’s intended length of stay and whether the applicant intends to remain permanently or become a United States citizen, and whether the applicant is inadmissible.”); and [8 U.S.C. § 1357\(c\)](#) (stating that CBPOs have “have power to conduct a search, without warrant, of the person, and of the personal effects in the possession of any person seeking admission to the United States, concerning whom such officer or employee may have reasonable cause to suspect that grounds exist for denial of admission to the United States under this chapter which would be disclosed by such search”). In performing their lawful functions, CBPOs are not required to provide *Miranda* warnings to travelers at the border before conducting routine questioning. *See United States v. Layne*, [973 F.2d 1417, 1420](#) (8th Cir. 1992) (citations omitted); *United States v. Blackwell*, [2018 WL 6804803](#), at \*5 (D. Minn. Dec. 27, 2018); *United States v. Intarathong*, [2021 WL 8082965](#), at \*9 (D. Minn. Dec. 30, 2021), *report and recommendation adopted*, [2022 WL 602234](#) (D. Minn. Mar. 1, 2022). That is because a temporary detention of a traveler during routine border inspections is not an arrest. *United States v. Oyekan*, [786 F.2d 832, 839 n.12](#) (8th Cir. 1986) (citation omitted). Even when an individual is under investigation for



criminal activity, customs officials are not required to provide *Miranda* warnings before conducting routine questioning. See *United States v. Unpradit*, [2018 WL 4483682](#), at \*5 (D. Minn. May 14, 2018) (“While Defendant was already under investigation concerning a sex trafficking organization, she was not asked about that investigation ... Because this examination did not stray beyond routine border questioning, no *Miranda* warning was required.”) (citation omitted), *report and recommendation adopted*, [2018 WL 3377177](#) (D. Minn. July 1, 2018), *appeal filed sub nom. United States v. Pawinee Unpradit*, No. 20-1825 (8th Cir. Apr. 20, 2020).

Here, CBPOs conducted a routine border inspection wherein they asked the defendant general questions, searched his luggage and sought the passwords to the defendant’s electronic devices.<sup>11</sup> CBPOs did not ask the defendant about Kingdom or any other specific criminal activity. Accordingly, because the defendant was subject to routine border questioning by CBPOs and not custodial interrogation triggering *Miranda* requirements, defendant’s motion to suppress statements made to CBPOs as violations of his Fifth Amendment rights should be denied.

**2. The Defendant Was Not In Custody When He Voluntarily Joined Federal Agents In An Open Conference Room And Waited For An Interpreter**

An individual is entitled to *Miranda* warnings only when he is interviewed by law enforcement while “in custody,” meaning there has been a “formal arrest or restraint on freedom of movement of the degree associated with a formal arrest.” *California v. Beheler*, [463 U.S. 1121, 1124–25](#) (1983); *United States v. LeBrun*, [363 F.3d 715, 720](#) (8th Cir. 2004) (en banc), *cert. denied*,

---

<sup>11</sup> Routine inspections may include manually searching travelers’ electronic devices. See CBP Directive No. 3340-049A, *Border Searches of Electronic Devices*, § 5.1.3 (Jan. 4, 2018); see also *United States v. Mendez*, [103 F.4th 1303, 1310](#) (7th Cir. 2024) (there is a “consensus among circuits that brief, manual searches of a traveler’s electronic device are ‘routine’ border searches requiring no individualized suspicion.”).

543 U.S. 1145, 125 S.Ct. 1292, 161 L.Ed.2d 105 (2005). In determining whether a person is “in custody” for Miranda purposes where there has been no formal arrest, a reviewing court must consider “the totality of the circumstances,” focusing on “the objective circumstances” and not the “subjective views harbored by either the interrogating officers or the person being questioned.” *Stansbury v. California*, 511 U.S. 318, 322-23 (1994); *United States v. Huether*, 673 F.3d 789, 794 (8th Cir. 2012) (quotation omitted). The Eighth Circuit often relies upon the *Griffin* factors to determine whether a person is in custody for Miranda purposes:

(1) [W]hether the suspect was informed at the time of questioning that the questioning was voluntary, that the suspect was free to leave or request the officers to do so, or that the suspect was not considered under arrest; (2) whether the suspect possessed unrestrained freedom of movement during questioning; (3) whether the suspect initiated contact with authorities or voluntarily acquiesced to official requests to respond to questions; (4) whether strong arm tactics or deceptive stratagems were employed during questioning; (5) whether the atmosphere of the questioning was police-dominated; or, (6) whether the suspect was placed under arrest at the termination of the questioning.

*United States v. Aldridge*, 664 F.3d 705, 711 (8th Cir. 2011) (citing *United States v. Griffin*, 922 F.2d 1343, 1349 (8th Cir. 1990)). The presence of the first three *Griffin* factors mitigate against the existence of custody, while the presence of the last three factors aggravate toward the existence of custody. *United States v. Axsom*, 289 F.3d 496, 500–01 (8th Cir. 2002). However, the Eighth Circuit has recently questioned whether a post-questioning arrest is particularly relevant under an objective inquiry. See *United States v. Treanton*, 57 F.4th 638 (8th Cir. 2023).

Although “a particularly strong showing with respect to one factor may compensate for a deficiency with respect to other factors,” *Griffin*, 922 F.2d at 1349, no one factor is dispositive, *United States v. Willie*, 462 F.3d 892, 896 (8th Cir. 2006). Nor must all factors weigh in the defendant’s favor for courts to decide that he was in custody. *United States v. Ollie*, 442 F.3d

1135, 1137–38 (8th Cir. 2006) (*citing United States v. Axsom*, 289 F.3d 496, 501 (8th Cir.2002)).

The Eighth Circuit has cautioned that “[t]he debatable marginal presence of certain judicially-created factors that ostensibly tend to ‘aggravate the existence of custody’ cannot create the functional equivalent of formal arrest where the most important circumstances show its absence.” *United States v. Czichray*, 378 F.3d 822, 828 (8th Cir. 2004). “The ultimate inquiry must always be whether the defendant was restrained as though he were under formal arrest.” *Id.*

The defendant voluntarily followed plain-clothed members of the Investigative Team to a back area of the airport to talk. There, the defendant sat down at a conference table in an open area. The defendant was not placed in handcuffs nor was he otherwise restrained. None of the agents displayed a weapon. The agents offered the defendant water and medicine. The agents told the defendant that he could make a phone call. The defendant was allowed to get up and use the bathroom. The defendant never asked if he was under arrest, and the agents did not tell him he was under arrest. The agents also did not use any strong-arm tactics during this period of questioning; in fact, the agents made clear on multiple occasions that they preferred to delay their conversation entirely until they could find a suitable interpreter.

When the defendant first sat down at the conference table, he made a spontaneous and unsolicited statement regarding his devices. This is not a statement made subject to interrogation. *See United States v. Crisolis-Gonzalez*, 742 F.3d 830, 837 (8th Cir. 2014) (*quoting United States v. Hayes*, 120 F.3d 739, 744 (8th Cir. 1997)) (“*Miranda* does not protect an accused from a spontaneous admission made under circumstances not induced by the investigating officers or during a conversation not initiated by the officers.”). In fact, for the first 1 hour and 16 minutes of the encounter, the defendant was asked only four substantive questions. These questions followed up the defendant’s unsolicited statement to agents regarding his devices. Over this initial

time period, the agents did not reference any criminal investigation or conduct. After the defendant answered these four questions, approximately 12 minutes into the encounter, the agents stopped the interview entirely until they could find an interpreter. For the next hour or so after that, the agents did not ask the defendant any questions at all other than what languages he could understand. These questions were cabined to their efforts to find a suitable interpreter.

Based on the foregoing, and in applying the *Griffin* factors, the defendant was not in custody for this initial portion of the interview. As such, he was not entitled to receive any *Miranda* warnings and his statements should not be suppressed based on a failure to provide them.

**3. The *Miranda* Warnings Provided to the Defendant Do Not Violate *Missouri v. Seibert* and the Defendant's Post-*Miranda* Statements Are Admissible**

As discussed above, the defendant was not in custody while he sat with agents waiting for an interpreter to join. Once an interpreter became available, the agents provided the defendant with his *Miranda* rights, both verbally and in writing. The defendant stated that he understood his rights, he signed a written form, and agreed to speak with agents.

The defendant argues that the agents employed a “two step interrogation” that was made unlawful by *Missouri v. Seibert*, 542 U.S. 600 (2004). In *Seibert*, the Supreme Court found that an officer's deliberate tactic of first questioning a subject without *Miranda* warnings, then later giving the warnings and repeating the questions already answered, made the subject's *Miranda* waiver invalid and, thus, the post-warning statements inadmissible. *Seibert*, 532 U.S. at 620; *United States v. Briones*, 390 F.3d 610, 613 (8th Cir. 2004). The Supreme Court delineated a list of factors for courts to consider in determining whether *Miranda* warnings delivered midstream are effective – the court must address (1) the extent of the first round of interrogation; (2) the extent to which the first and second rounds on interrogation overlap; (3) timing and setting of both

questioning sessions, including whether a continuity of police personnel existed; and (4) the extent to which the interrogator's questions treated the second round as continuous with the first. *Seibert*, 532 U.S. at 620; *United States v. Aguilar*, 384 F.3d 520, 524 (8th Cir. 2004).

Yet, the threshold issue, which the Government must prove by a preponderance of the evidence, is whether an officer's interrogation technique was a “designed,” “deliberate,” or “calculated” circumvention of *Miranda*. *United States v. Black Bear*, 422 F.3d 658, 664 (8th Cir.2005), *citing Seibert*, 542 U.S. at 618 (Kennedy, J., concurring); *United States v. Ollie*, 442 F.3d 1135, 1142–43 (8th Cir. 2006); *United States v. Hernandez-Hernandez*, 384 F.3d 562, 566 (8th Cir. 2004) (finding no violation where the failure to read a subject his rights did not seem to have been “an intentional withholding that was part of a larger, nefarious plot”). Where officers make no calculated effort to elicit a confession and the subject makes no incriminating statements, there is no “two part interrogation.” *United States v. Wise*, 588 F.3d 531, 536 (8th Cir. 2009). Nor is there a “two part interrogation” where the two questioning sessions are separated by time and location. *United States v. Walker*, 518 F.3d 983, 985 (8th Cir. 2008). Nor is there a “two step interrogation” where the pre-warning conversation is “brief and narrow in scope,” is polite and conversational, and the officer does not question the subject about their involvement in criminal conduct. *United States v. Jones*, 70 F.4th 1109, 1114 (8th Cir.), *cert. denied*, 144 S. Ct. 366 (2023).

The defendant's reliance on *Missouri v. Seibert* is misplaced as there is no evidence that agents utilized a deliberate or calculated interrogation technique to elicit a confession. At no point during the first part of the interview did agents reference the fact that there was a criminal investigation involving the defendant or Kingdom. In fact, the agents did not question the defendant at all about his involvement in criminal conduct, nor did they make any attempt to elicit a confession from the defendant. The agents remained polite and conversational and asked only

four follow up questions to the defendant's spontaneous statement about his devices. As such, this pre-*Miranda*-warning stage of the interview was extremely narrow in scope. Although the *Miranda* warnings were not given until 1 hour and 16 minutes into the encounter, the majority of that time was spent searching for an interpreter and not related to actual questioning of the defendant.

Based on the foregoing, the agents did not deliberately delay administering *Miranda* warnings to the defendant to elicit a confession. As such, the defendant's post-*Miranda* statements are admissible and should not be suppressed.

**4. The Defendant Knowingly, Intelligently and Voluntarily Waived His *Miranda* Rights**

The defendant validly waived his *Miranda* rights, and thus, there is no basis for suppression of his post-*Miranda* statements. A defendant's agreement to waive his Fifth Amendment right against self-incrimination must be knowing, intelligent, and voluntary. *Miranda v. Arizona*, 384 U.S. 436, 444 (1966). A waiver is knowing and intelligent if it is "made with a full awareness of both the nature of the right being abandoned and the consequences of the decision to abandon it." *United States v. Syslo*, 303 F.3d 860, 865 (8th Cir. 2002); *United States v. Gallardo*, 495 F.3d 982, 990 (8th Cir. 2007). A waiver is made voluntarily if "it was the product of a free and deliberate choice rather than intimidation, coercion, or deception." *Moran v. Burbine*, 475 U.S. 412, 421 (1986). To determine whether a waiver or a confession was voluntary, a court looks at the totality of the circumstances to determine whether the individual's will was overborne. *Gallardo*, 495 F.3d 982, 990. The burden is on the Government to show the waiver was valid by a preponderance of the evidence. *Black Bear*, 422 F.3d at 663.

Where a subject is advised of his *Miranda* rights through an interpreter, the mere fact that a law enforcement agent or employee acts as the interpreter does not make a *Miranda* waiver

involuntary or coercive. *Carrion v. Butler*, [835 F.3d 764, 776](#) (7th Cir. 2016); *United States v. Lind*, [542 F.2d 598, 599](#) (2d Cir. 1976). In addition, the fact that an interpreter translates the defendant's rights to him in his native tongue over the phone has no effect on the sufficiency of the waiver where it is clear the defendant adequately understands what is being said. *United States v. Castro-Higuero*, [473 F.3d 880, 886](#) (8th Cir. 2007). A defendant's waiver is valid where he communicates easily with agents, does not express any lack of understanding, and does not ask agents to stop. *United States v. Garcia*, [189 F. Supp. 3d 826, 829](#) (S.D. Iowa 2016).

The defendant told agents that he understood the Czech language and he agreed to proceed with an interview interpreted to him in the Czech language. The defendant also signed a written waiver that was translated for him. An interpreter participated through a phone call, and the defendant appeared to understand the questions as they were interpreted to him. Throughout the interview, the defendant provided responsive answers to questions. At no point did the defendant state that he did not understand anything that was interpreted to him. As such, the defendant's waiver was made knowingly, intelligently and voluntarily.

**C. Evidence Obtained from the Defendant's Devices Should Not Be Suppressed**

The defendant argues that CBP did not have authority to search his electronic devices pursuant to the border search doctrine without a warrant. As discussed below, CBP is not required to have reasonable suspicion to perform a basic search of the defendant's electronic devices, let alone probable cause or a warrant. In any event, CBP had reasonable suspicion to search the defendant's electronic devices based on the information provided by HSI, prior to the defendant's arrival, that the defendant was the suspected administrator of a marketplace on the dark web, which allegedly facilitates sales to the United States of stolen identities, narcotics, counterfeit currency, and stolen/fraudulent identities. In addition, the Government did, in fact, later obtain a search

warrant for the defendant's devices. As discussed below, the Devices Warrant was supported by ample probable cause and was not overbroad.

**1. The Search of the Defendant's Devices at the Airport Was Permissible Under the Border Search Doctrine**

The defendant argues that the seizure of his electronic devices by CBP exceeded the permissible limits of a border search because 1) the underlying and primary objective was criminal, not immigration or customs enforcement, and 2) the items seized were electronic devices.

Border searches are a “longstanding, historically recognized exception to the Fourth Amendment’s general principle that a warrant be obtained” for a search. *United States v. Ramsey*, 431 U.S. 606, 621 (1977); *see also* 19 U.S.C. § 1582 (“all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under [customs] regulations.”) and 19 U.S.C. § 482 (stating that customs agents may “stop, search, and examine” any “vehicle, beast or person” suspected of carrying contraband). In fact, border searches are inherently reasonable “simply by virtue of the fact that they occur at the border.” *Ramsey*, 431 U.S. at 616. Protecting territorial integrity is of paramount interest to a sovereign nation and warrantless border searches serves the need for “national self-protection.” *Carroll v. United States*, 267 U.S. 132, 154 (1925); *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004); *see also* *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (“Consistently, therefore, with Congress’ power to protect the Nation by stopping and examining persons entering this country, the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.”)



The defendant primarily argues that electronic devices are not subject to border searches, citing *Riley v. California*, 573 U.S. 373 (2014). *Riley* put an end to the general practice of warrantless searches of cellphones incident to arrest, holding that a warrant is required. The rationale of *Riley* was that modern cellphones hold “the privacies of life” and are thus entitled to protection exceeding the warrant exception for searches incident to arrest.

The defendant argues that the rationale of *Riley* should be extended to limiting border searches. This very argument was recently considered and rejected by the Eighth Circuit in *United States v. Xiang*, 67 F.4th 895 (8th Cir. 2023). *Xiang* involved a border search of electronic devices at an airport as Xiang was leaving the United States. The court rejected Xiang’s assertions that *Riley*’s rationale extends to border searches as “a misapprehension of the applicability of *Riley*,” noting that “[n]o Circuit has held that the government must obtain a warrant to conduct a routine border search of electronic devices.” *Xiang*, 67 F.4th at 900.

As *Xiang* recognizes, the border search doctrine is markedly different from the search-incident-to-arrest exception to the Fourth Amendment warrant requirement at issue in *Riley*. See, e.g., *United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019) (“here we deal with the border search exception - not the search incident to arrest exception - and the difference in context is critical”); *United States v. Laynes*, 481 F. Supp. 3d 657, 664 (S.D. Ohio 2020). The search-incident-to-arrest exception permits a warrantless search of the person and the immediate vicinity of the arrestee for the limited purpose of locating any weapons that might endanger the arresting officer and to prevent the destruction of evidence. See *Riley*, 573 U.S. at 383. “[T]here are no comparable risks” of harm to the arresting officer or destruction of evidence “when the search is of digital data.” *Id.* at 386.

The border search doctrine, by contrast, serves different and broader purposes, including protecting the nation’s core sovereignty in controlling the entry and exit of persons and property to protect national security and to detect threats to the citizenry. *See, e.g., United States v. Udofot*, [711 F.2d 831, 839](#) (8th Cir. 1983). Unlike with searches incident to arrest, the purposes underlying the border search doctrine apply with full force to searches of electronic media, which can contain child pornography or harmful data in any number of ways including stolen material that would facilitate economic espionage against the United States. *See, e.g., United States v. Tousey*, [890 F.3d 1227, 1235](#) (11th Cir. 2018) (“digital child pornography poses the same exact ‘risk’ of unlawful entry at the border as its physical counterpart”). In short, “*Riley* did not diminish the Government’s interest in protecting the border or the scope of the border search exception,” *United States v. Saboonchi*, [48 F. Supp. 3d 815, 819](#) (D. Md. 2014), because “warrantless electronic device searches are essential to the border search exception’s purpose of ensuring that the executive branch can adequately protect the border,” *Alasaad v. Mayorkas*, [988 F.3d 8, 17](#) (1st Cir. 2021); accord *United States v. Wanjiku*, [919 F.3d 472, 484](#) (7th Cir. 2019) (explaining that neither *Riley* nor *Carpenter v. United States*, [138 S. Ct. 2206](#) (2018), “addresses searches at the border where the government’s interests are at their zenith”). A warrant requirement “would hamstring the [government’s] efforts to prevent border-related crime and protect this country from national security threats.” *Alasaad*, [988 F.3d at 17](#).

Every circuit court to consider the matter has agreed with *Xiang* and concluded that the border search doctrine permits the warrantless search of electronic devices such as computers and cellphones. *Alasaad*, [988 F.3d](#), at 16-21; *United States v. Linarez-Delgado*, [259 F.App’x 506, 508](#) (3d Cir. 2007); *United States v. Ickes*, [393 F.3d 501, 505-06](#) (4th Cir. 2005); *United States v. Castillo*, [70 F.4th 894, 898](#) (5th Cir. 2023); *United States v. Stewart*, [729 F.3d 517, 525-26](#) (6th

Cir. 2013); *United States v. Cotterman*, [709 F.3d 952, 960-68](#) (9th Cir. 2013) (en banc); *United States v. Williams*, [942 F.3d 1187, 1190](#) (10th Cir. 2019), *cert. denied*, [141 S. Ct. 235](#) (2020); *United States v. Touset*, [890 F. 3d 1227, 1231-37](#) (11th Cir. 2018); *see also United States v. Molina-Isidoro*, [884 F.3d 287, 292-93](#) (5th Cir. 2018) (affirming denial of motion to suppress and stating that no court has “required a warrant even for forensic searches [of electronic devices] occurring at the border”); *United States v. Wanjiku*, [919 F.3d 472, 486-88](#) (7th Cir. 2019) (affirming denial of motion to suppress and stating that “agents acted lawfully because they possessed reasonable suspicion” that “a search of [defendant’s] electronic devices would reveal evidence of criminal activity involving minors”) (quotation marks omitted). As the Seventh Circuit explained, “[n]o court has ever required more than reasonable suspicion for a border search” of an electronic device or anything else. *United States v. Skaggs*, [25 F.4th 494, 500](#) (7th Cir. 2022); *accord Alasaad*, [988 F.3d at 17-18](#) (“Every circuit that has faced this question” has held “that neither a warrant nor probable cause is required for a border search of electronic devices.”). The defendant has offered no reason to disturb this well-established law.

While the Ninth Circuit in *United States v. Cano*, [934 F.3d 1002](#) (9th Cir. 2019) *has* made a distinction between manual and forensic searches of digital devices at the border, the defendant has ridiculed the distinction as “factually meaningless and constitutionally unworkable.” Motion, at 21. *Cano* involved a defendant arrested at the Mexican border for smuggling 14 kilograms of cocaine. An HSI agent manually searched Cano’s cellphone and then conducted a forensic search of it without a warrant. The Ninth Circuit held “that manual searches of cellphones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cellphone requires a showing of reasonable suspicion.” *Cano*, [934 F.3d at 1016](#); *but see United States v.*

*Touset*, [890 F.3d 1227, 1231](#) (11th Cir. 2018). Notably, *Cano* did not require a showing of probable cause or insist on a warrant to conduct a forensic search.

Rejecting *Cano* leaves the defendant in an all or nothing stance, that a warrant should be (not is) required for all border searches of electronic devices. Of course, the fact that in this case agents obtained a search warrant for a forensic search of the defendant's devices after a very brief manual search of his cellphone forces the defendant into this extreme position. In short, the defendant is asking this court to ignore a century long precedent that has been continually reaffirmed by the Supreme Court and Circuit Courts. *United States v. Mendez*, [103 F.4th 1303, 1307](#) (7th Cir. 2024) (*Riley* does not support “altering the long-settled rule exempting border searches from warrant and probable cause requirements.”).

The defendant also posits that “the Fourth Amendment only permits border searches tied to enforcement of immigration and customs laws.” Motion, at 21. This assertion was also made in *Xiang* and summarily rejected by the Eighth Circuit, citing to *Alasaad v. Mayorkas*, [988 F.3d 8](#) (1st Cir. 2021); *Xiang*, [67 F.4th at 200](#). *Alasaad* addressed the very same argument as defendant's. After affirming that border searches are routine and need not be supported by reasonable suspicion, and are not limited in scope, the court held that “border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced by CBP or ICE.” *Alasaad*, [988 F.3d at 21](#).

“This is so because the government's interest in preventing crime at international borders ‘is at its zenith’ (*Ramsey*, [431 U.S. at 616](#)) and it follows that a search for evidence of either contraband or a cross-border crime furthers the purposes of the border search exception to the warrant requirement.” *Alasaad*, [988 F.3d at 19](#). Other circuits have also held that the validity of warrantless border searches “does not depend on whether it is prompted by a criminal investigative

motive.” *United States v. Levy*, [803 F.3d 120, 123](#) (2d Cir. 2015); *United States v. Gust*, [471 F.3d 144, 149](#) (D.C. Cir. 2006); *United States v. Castillo*, [70 F.4th 894](#) (5th Cir. 2023); *United States v. Cano*, [934 F.3d 1002, 1013](#) (9th Cir. 2019). In fact, “[n]o circuit has held that the government must obtain a warrant to conduct a routine border search of electronic devices.” *Xiang*, [67 F.4th at 900](#). Defendant’s insistence that this court hold differently from every Circuit, including the Eighth, to consider the issue is not tenable.

## **2. The Devices Warrant Is Supported by Ample Probable Cause<sup>12</sup>**

Probable cause is defined as a “fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Warford*, [439 F.3d 836, 841](#) (8th Cir. 2006) (quoting *Illinois v. Gates*, [462 U.S. 213, 238](#) (1983)). A totality of the circumstances test is used to determine whether probable cause exists. *United States v. Oropesa*, [316 F.3d 762, 768](#) (8th Cir. 2003); *United States v. Notman*, [831 F.3d 1084, 1088](#) (8th Cir. 2016). Courts should apply a common-sense approach and consider all relevant circumstances to determine whether probable cause exists. *United States v. Buchanan*, [167 F.3d 1207, 1211](#) (8th Cir. 1999). The affidavit should not be examined in a “hypertechnical fashion.” See *United States v. Solomon*, [432 F.3d 824, 827](#) (8th Cir.2005) (quoting *United States v. Williams*, [10 F.3d 590, 593](#) (8th Cir.1993); see also *Florida v. Harris*, [568 U.S. 237, 243](#) (2013) (totality-of-the circumstances tests are “not readily, or even usefully, reduced to a neat set of legal rules”).

---

<sup>12</sup> As to both the Devices Warrant and the Google Warrants (discussed below), the bulk of the defendant’s argument as to the deficiency of the warrants is based on his perception that the Government’s clustering analysis is unreliable. See Motion, at 37. The defendant argues that, even if the clustering analysis is accurate, the results only show that the defendant had repeated transactions with an administrator of Kingdom and not that these were related to the operation of Kingdom. *Id.* at 38. The defendant then states that “[i]t can be assumed that [defendant] was likely a regular user of Kingdom Marketplace and paid the Kingdom Marketplace Administrator for using Kingdom Marketplace’s services.” *Id.* at 39. This argument appears to suggest that the defendant was involved in the criminal activity for which Kingdom Marketplace was the forum, thus, amplifying the probable cause set forth in the affidavits.

“When the [issuing judge] relied solely upon the supporting affidavit to issue the warrant, ‘only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause.’” *United States v. Etheridge*, 165 F.3d 655, 656 (8th Cir. 1999) (*quoting United States v. Gladney*, 48 F.3d 309, 312 (8th Cir. 1995)). In assessing probable cause for a warrant, a reviewing court must “pay great deference to the probable cause determinations of the issuing judge or magistrate, and [the] inquiry is limited to discerning whether the issuing judge had a substantial basis for concluding that probable cause existed.” *United States v. Daigle*, 947 F.3d 1076, 1081 (8th Cir. 2020) (citations and quotations omitted); *see also United States v. Green*, 954 F.3d 1119, 1123 (8th Cir.) (“We owe great deference to the issuing court’s probable-cause determination.”) (citation omitted), *cert. denied*, 141 S. Ct. 597 (2020). Where the issuing judge had a “substantial basis” for concluding the “search would uncover evidence of wrongdoing,” the reviewing court must uphold the probable cause determination. *United States v. Horn*, 187 F.3d 781, 785 (8th Cir. 1999).

Here, the affidavit supporting the Devices Warrant has ample probable cause that the defendant committed specific federal crimes and that evidence of those crimes would be found on his electronic devices. The affidavit discussed numerous and significant links between the defendant’s various online accounts and Kingdom. For example, the affidavit stated that a specific IP address used to access Kingdom’s reddit account was also used to access the defendant’s cryptocurrency accounts, which received large amounts of cryptocurrency from Kingdom (paragraphs 30 to 44). In addition, the affidavit provided detail showing that the defendant’s various bank accounts received numerous, large, unexplained cash deposits over the period of time that Kingdom was operating (paragraphs 45 to 49). In addition, the affidavit discusses the results of the lawful searches of the defendant’s Google account (Alan.vs.Bill@gmail.com) and

Kingdom's Reddit accounts, which show significant links to Kingdom and its back-end infrastructure and cryptocurrency accounts (paragraphs 64 to 69).

HSI SA Kraft's affidavit further describes how Kingdom operated continuously, including at times when the defendant travelled across the world (paragraph 76). The affidavit further states that the defendant used an Apple iPhone on the AT&T network when he was in the United States in January 2023, including at a time when Kingdom had experienced a DDoS attack and Kingdom administrators were actively posting messages to its users (paragraph 80). The affidavit then provides evidence from a search of the defendant's Apple iCloud account that the defendant used numerous encrypted communication applications during this same time period (paragraphs 70 to 75). As set forth in the affidavit, each of the defendant's seized devices were capable of accessing the internet and running the programs known to be used to operate Kingdom (paragraphs 80 and 82).

Based on the evidence set forth in the affidavit for the Devices Warrant, there was ample probable cause to search each of the defendant's devices.

### **3. The Device Search Warrant Is Sufficiently Particular and Is Not Overbroad**

Warrants must state with particularity the scope of the authorized search. *Kentucky v. King*, 563 U.S. 452, 459 (2011). To satisfy the particularity requirement of the fourth amendment, a warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized. *United States v. Summage*, 481 F.3d 1075, 1079 (8th Cir. 2007) (citing *United States v. Strand*, 761 F.2d 449, 453 (8th Cir.1985)). The degree of specificity required will depend on the circumstances of the case and on items involved. *United States v. Horn*, 187 F.3d 781, 788 (8th Cir. 1999). Warrants related to complex criminal schemes "may be deemed

sufficient even though they are less particular than warrants pertaining to more straightforward criminal matters.” *United States v. Allen*, [2018 WL 1726349](#), at \*6 (D. Kan. Apr. 10, 2018).

The particularity requirement is one of “practical accuracy rather than” of hypertechnicality. *United States v. Sigillito*, [759 F.3d 913, 923](#) (8th Cir. 2014) (quoting *United States v. Peters*, [92 F.3d 768, 769–70](#) (8th Cir.1996); see also *United States v. Fiorito*, [640 F.3d 338, 346](#) (8th Cir. 2011) (cleaned up) (quoting *Milliman v. Minnesota*, [774 F.2d 247, 250](#) (8th Cir. 1985)) (“Whether a warrant fails the particularity requirement cannot be decided in a vacuum,” and we must consider “the total circumstances surrounding the case.”). A warrant affidavit may provide the necessary particularity if it is attached to the warrant. *United States v. Nieman*, [520 F.3d 834, 839](#) (8th Cir. 2008). The Eighth Circuit has consistently held that warrants that authorize the seizure of “evidence and fruits of violations” of specific federal statutes provide a “specific limitation” and sufficient particularity to satisfy the Fourth Amendment. See, e.g., *United States v. Nieman*, [520 F.3d 834, 839](#) (8th Cir. 2008); *United States v. Coleman*, [909 F.3d 925, 931](#) (8th Cir. 2018) (affirming validity of warrant authorizing search and seizure of “books, records, receipts, ledgers, and other papers related to ... controlled substances”); *Fiorito*, [640 F.3d at 346–47](#) (affirming denial of motion to suppress despite language authorizing seizure of “[e]ntire files” because the broad language was cabined by specific categories of information to be searched and seized).

Here, the Devices Warrant clearly states what was sought to be searched and seized and the scope of the warrant is supported by probable cause. As such, the Devices Warrant is both sufficiently particular and is not overbroad. First, the standard of “practical accuracy” is met here. See *Sigillito*, [759 F.3d at 923](#) (quoting *Peters*, [92 F.3d at 769–70](#)). In light of the facts and circumstances of the investigation, the warrant is sufficiently particular, placing a specific



limitation on the search and enabling officers to identify what evidence was to be seized. Attachment B to the warrant clearly states that the warrant authorizes the seizure of records that “relate to violations of 18 U.S.C. Sections 371 (conspiracy), 1543 (forgery or false use of passport), 1028 (identity theft), 1029 (access device fraud), 1956 and 1957 (money laundering); 21 U.S.C. Sections 841 and 846 (drug offenses) (“TARGET OFFENSES”) and involve Alan BILL from January 2020 to Present.” Attachment B then lists a number of specifically identified items that are directly related to the criminal investigation as set forth in the affidavit. For example, Attachment B references items such as: Information that constitutes evidence related to the use of the monikers “vend0r”, “Papinian3”, “kingdommarketofficial” and “OhLongJohnson”; The infrastructure of Kingdom Market; and Information that constitutes evidence concerning the access, creation or maintenance of websites and hidden (Tor-based) services.

The defendant fails to cite any precedent supporting suppression of evidence where the warrant was as detailed and specific as that in the present case. Based on the foregoing, the Device Search Warrant is sufficiently particular and is not overbroad.

**D. The Google Warrants Should Not Be Suppressed**

As described above, Judge Mensah issued the First Google Warrant in September 2023 and Judge Collins issued the Second Google Warrant in December 2023. The defendant does not specify which warrant that he claims is deficient.<sup>13</sup> In any event, both Google Warrants are supported by ample probable cause and both are sufficiently particular and not overbroad.

**1. The Google Warrants Are Supported By Ample Probable Cause**

As with the Devices Warrant, both of the Google Warrants are supported by ample probable cause that the defendant committed federal crimes and that evidence of those crimes

---

<sup>13</sup> See footnote 11.

would be found within his Google Account. This Court should apply a common-sense approach and not examine the sufficiency of the warrants in a “hypertechnical fashion.” *See Buchanan*, 167 F.3d at 1211; *Solomon*, 432 F.3d at 827. This Court should also pay great deference to the issuing judges for each of the Google Warrants. *See Daigle*, 947 F.3d at 1081; *Green*, 954 F.3d at 1123.

Here, the affidavits supporting the Google Warrants discussed numerous and significant links between the defendant’s various online accounts and Kingdom. For example, the affidavit for the First Google Warrant describes specific links between Kingdom cryptocurrency accounts and two of the defendant’s cryptocurrency accounts, both of which listed the defendant’s Google account as the associated email address (paragraphs 40 to 45). The affidavit explained that the defendant used his Google account on travel records to the United States in 2018 (paragraph 46). The affidavit then explained that the results from a 18 U.S.C. § 2703(d) order included non-content records showing that the defendant’s Google Account had received numerous email messages from cryptocurrency services such as crypto.com, coinstats.app and LocalMonero (paragraphs 49 to 52). Finally, the affidavit described in detail specific transactions wherein the defendant’s cryptocurrency accounts were used to make a payment from Kingdom to a third-party service provider (paragraphs 53 to 58).

Similarly, the affidavit for the Second Google Warrant included significant additional information connecting the defendant and the Google Account to criminal activity, all of which was discovered through the execution of the First Google Warrant. Specifically, the affidavit states that results from the first search showed: images and videos that included the name “Vend0r” on them (paragraph 62); a video file showing an individual performing administrative functions on Kingdom (paragraphs 63 to 67); internet image and keyword searches for “kingdom Market”, “server housing” and “Litecoin icon” before Kingdom existed (paragraph 69); and numerous files

showing recovery information and seed phrases for cryptocurrency accounts, IP masking tools and encrypted cloud storage and file hosting services, including ones that have a direct link to Kingdom (paragraphs 70 to 72).

Based on the evidence set forth in the affidavits for the Google Warrants, there was ample probable cause to search the defendant's Google Account.

## **2. The Google Warrants Are Sufficiently Particular and Are Not Overbroad**

As with the Devices Warrant, the Google Warrants clearly stated what was sought to be searched and seized and the scope of the warrant was supported by probable cause. For each of the Google Warrants, Attachment B clearly states that the warrant authorizes the seizure of records that relate to specific crimes, specific dates, that involve the defendant, and that relate to specifically identified items that are directly related to the criminal investigation as described and set forth in the affidavits. As such, the Google Warrants were both sufficiently particular and not overbroad. *See, e.g., United States v. Ulbricht*, [858 F.3d 71, 104](#) (2d Cir. 2017) (finding the warrant to search a defendant's Google account was not overbroad because it listed the offenses to be investigated, things to be searched, and information to be seized); *United States v. Allen*, [2018 WL 1726349](#), at \*6 (D. Kan. Apr. 10, 2018) (finding that a warrant to search the defendant's Facebook account was not overbroad because it was limited to gathering evidence of a specified crime which by its nature required a broad search).

## V. **Conclusion**

For the foregoing reasons, the United States respectfully requests that Defendant's Motion to Suppress Evidence ([Doc. 98](#)) be denied in its entirety.

Respectfully submitted,

SAYLER A. FLEMING  
United States Attorney

/s/ Kyle T. Bateman  
KYLE T. BATEMAN, #996646DC  
Assistant United States Attorney  
111 South Tenth Street, Room 20.333  
Saint Louis, Missouri 63102  
(314) 539-2200

**CERTIFICATE OF SERVICE**

I hereby certify that, on November 8, 2024, the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon all counsel of record.

s/ Kyle T. Bateman

KYLE T. BATEMAN, #996646DC

Assistant United States Attorney